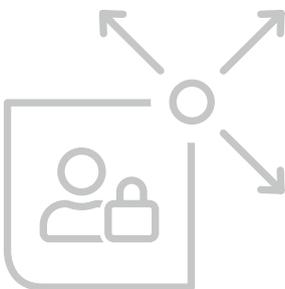


From Zero to Hero

CIAM – Ein Spagat zwischen Sicherheit und Customer Experience



Virtueller Roundtable mit Enterprise-Kunden lotet die Herausforderungen und Potenziale ganzheitlicher Identity und Access Management Plattformen aus.

Im Fokus der Diskussion:

- **Wie sich IAM und CIAM abgrenzen lassen**
- **Die Chancen und Herausforderungen von CIAM**
- **Hub-and-Spoke für Enterprise-Umgebungen**
- **Integration bestehender IAM-Lösungen**
- **Governance und Datenschutz**

Die Digitalisierung des privaten und des beruflichen Lebens schreitet rasant voran: Über nahezu alle Branchen hinweg wird inzwischen weltweit digital und remote gearbeitet, online geshoppert und über das Web kommuniziert, konsumiert und kollaboriert. Die erste Welle der Ad-hoc-Digitalisierung nahmen die meisten Unternehmen im vergangenen Jahr mit Bravour – auch wenn die Umstellung hinter den Kulissen oft einen enormen Kraftakt erforderte. Doch nun gilt es, die unter Zeitdruck implementierten oder hochskalierten Systeme in einen stabilen, sicheren und Compliance-konformen Betrieb zu überführen – und das ist nicht zuletzt mit Blick auf die sichere Registrierung, Authentisierung und Autorisierung der Anwender alles andere als einfach. Hinzu kommen die Bedrohungen der Plattformbetreiber in puncto Angriffe.

Daher veranstaltete iC Consult im Februar 2021 einen virtuellen IAM Excellence Talk unter dem Titel „From Zero to Hero: CIAM – Ein Spagat zwischen Sicherheit und Customer Experience“, und lud global tätige Enterprise-Kunden zum offenen Meinungs- und Erfahrungsaustausch ein. Mit am Tisch: Identity Management Experten vom Herstellerpartner Okta. Solution Engineering Manager Götz Walecki moderierte die Diskussion, teilte Best Practices aus weltweiten Projekten und gab den Teilnehmern Tipps für die CIAM-Einführung in verteilten Umgebungen.

Im Rahmen der rund einstündigen Diskussion konzentrierten sich die Teilnehmer vorrangig auf sieben zentrale Fragestellungen, die ihre Unternehmen aktuell beschäftigen, und erarbeiteten gemeinsam mit Okta und iC Consult erste, auf Best Practices aufsetzende, Lösungskonzepte.



Wie sich IAM und CIAM abgrenzen lassen

1. Wir haben bereits ein Identity Access Management (IAM) für unsere Workforce implementiert. Das Customer Identity and Access Management (CIAM) kommt im Zuge der Digitalisierung als neues Thema hinzu. Wie lassen sich die beiden Projekte abgrenzen?

Die Teilnehmer waren einhellig der Meinung, dass IAM und CIAM in der Regel zwar ähnliche Ziele verfolgen – die sichere, bedienerfreundliche und Governance-konforme Authentisierung der User – aber in der Praxis erhebliche Unterschiede aufweisen. Die wichtigsten Unterschiede:

- Das **Onboarding** interner Mitarbeiter folgt ganz anderen Prozessvorgaben als etwa die Einbindung von Kunden an einen Online-Shop.
- Die **Nutzerdaten** befinden sich im Falle einer Mitarbeiterlösung in der Regel im HR-System und dann in einem dedizierten, zentralen Verzeichnis (meist: Microsoft Active Directory). Bei einem CIAM liegen sie häufig in CRM- und Sales-Datenbanken oder auf den Servern externer Dritter (Apple-ID) – oder müssen erst online abgefragt werden.
- Als **Authentisierungswerkzeuge** setzen die Teilnehmer bei ihren Workforce-IAMs heute auf starke Multifaktor-Authentisierung. Im CIAM-Umfeld gewinnen dafür Social-Authentication-Lösungen rasant an Bedeutung.
- Die **unterliegende Infrastruktur** von IAM und CIAM unterscheidet sich ebenfalls – während erstere zumeist auf HR-Systemen und Benutzerdatenbanken basieren, handelt es sich bei klassischen CIAM-Lösungen, so die Teilnehmer, in der Regel um Portallösungen.

In der Summe adressieren die Teilnehmer IAM und CIAM daher als separate Projekte mit unterschiedlichen Value-Drivern und Herausforderungen.



Die Chancen und Herausforderungen von CIAM

2. Die Teilnehmer geben an, dass CIAM bei ihnen derzeit in den Kinderschuhen steckt und im Vergleich zu IAM als aufwändiger wahrgenommen wird. Woher kommt der Eindruck?

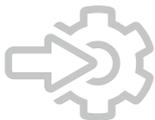
Ein Diskussionsteilnehmer bringt es auf den Punkt: IAM-Lösungen für die Workforce sind in der Regel maximal für einige Zehntausend Anwender ausgelegt, während CIAM-Lösungen häufig Millionen von Consumern sicher und Compliance-konform authentisieren müssen. Hinzu kommt, dass die Art der Zugriffe, die Herkunft der Nutzerdaten und die favorisierten Authentisierungswerkzeuge wesentlich stärker variieren und für die Corporate-IT schwerer zu kontrollieren sind. Addiert man dann noch das Risikopotenzial bei Governance-Verstößen und die hohen Usability-Anforderungen, ist klar, warum CIAM-Projekte häufig als enorme Herausforderung wahrgenommen werden. Andere Roundtable-Teilnehmer weisen aber darauf hin, dass CIAM in vielen Bereichen deutlich geringere Hürden aufweist: So müssten in der Regel weniger Anwendungen integriert und weniger Rollen verwaltet werden als bei Workforce-IAM-Lösungen. Damit sei CIAM durchaus als Einstieg in einige spannende Themenbereiche geeignet – etwa für Autorisierungsprojekte.



Hub-and-Spoke für Enterprise-Umgebungen

3. In Konzernen mit vielen Bereichen und internationalen Niederlassungen bergen IAM- und CIAM-Projekte besondere Herausforderungen. Lassen sich solche Strukturen mit einer einheitlichen Lösung abdecken?

Teilnehmer, die bereits Erfahrungen mit der Hub-and-Spoke-Architektur von Okta gemacht haben, bestätigen: Ja, das funktioniert. In diesem Modell gibt die Zentrale (das „Hub“) vor, welche Anwendungen in die Authentisierungslösung einzubinden sind. Die örtlich oder organisatorisch abgesetzten Divisions (die „Spokes“) entscheiden anschließend autark, welchen Mitarbeitern und mit welchen Vorgaben diese Anwendungen zur Verfügung gestellt werden sollen. Dieser Ansatz garantiert im Alltag ein hohes Maß an Flexibilität, so die Teilnehmer, und ist damit selbst für große Enterprise-Umgebungen sehr gut geeignet.



Integration bestehender IAM-Lösungen

4. Für welche Unternehmen lohnt es sich denn, das Thema CIAM anzugehen?

Betrachtet man das Tempo, mit dem die Virtualisierung voranschreitet, wird CIAM vom Nice-to-have mehr und mehr zum Must-have. Die Teilnehmer sind sich einig, dass eine solche Lösung mit Blick auf die Governance, die Sicherheit und den Datenschutz künftig weiter an Bedeutung gewinnen wird. Als besonders hoch bezeichnen sie den Mehrwert von CIAM, wenn es gelingt, die Lösung in vorhandene Marketing-, CRM- und Sales-Datenbanken zu integrieren. Dafür bedarf es aber, schon mit Blick auf die hohen Anwenderzahlen, einer umfassenden Automatisierung – der Reifegrade der Umsetzung muss also vergleichsweise hoch sein.

5. Ist es eine gute Idee, IAM und CIAM zu konsolidieren?

Die Roundtable-Teilnehmer neigen dazu, IAM und CIAM als getrennte Projekte anzugehen. Aktuell konzentrieren sich die meisten darauf, den Reifegrad ihrer IAM-Umgebungen voranzutreiben und im ersten Schritt ihren Mitarbeitern die Vorzüge dieser Lösungen zu erschließen. Nach eigener Aussage sehen sich viele derzeit noch in der Frühphase der Projekte (Reifegrad 1-2). Das Thema CIAM bezeichnen mehrere Teilnehmer ausdrücklich als „noch in den Kinderschuhen“. Die Runde sieht aber durchgängig das Potenzial der Technologie, gerade mit Blick auf die Social Authentication über Drittanbieter wie Apple-ID. Diese könnte sich, so der Tenor in der Runde, durchaus zu einem echten Wachstumstreiber entwickeln, da viele Kunden Single Sign-on und passwortlose Modelle schon jetzt favorisieren und als spürbaren Mehrwert wahrnehmen.

6. Lassen sich in unternehmensweiten IAM- oder CIAM-Initiativen auch historische Lösungen einbinden?

Die Runde gibt zu bedenken, dass heute nur die wenigsten IAM- oder CIAM-Projekte tatsächlich auf der grünen Wiese beginnen. Nahezu alle Unternehmen haben in diesem Bereich bereits Erfahrungen gesammelt, und die meisten haben auch Legacy-Systeme im Einsatz.

Wer sich heute für die Implementierung einer unternehmensweiten Identity und Access Management Lösung entscheidet, hat in der Regel den Wunsch:

- seine Bestandssysteme einzubinden;
- das Identity Management zu zentralisieren;
- die Compliance und Governance auf eine einheitliche Basis zu stellen; und
- die Prozesse zusammenzuführen.

An dieser Stelle melden sich erneut die Teilnehmer mit Hub-and-Spoke-Erfahrung (siehe oben) zu Wort, und betonen, dass eine solche enge Integration mit Okta durchaus realisierbar ist: Die Okta Lösungen lassen sich bei Bedarf jederzeit als hoheitliches System im Backend implementieren, um vorgeschaltete Legacy-Systeme in einer Plattform zusammenzuführen und (vom Anwender unbemerkt) zu koordinieren. In einer solchen Umgebung steht den Unternehmen auch die Möglichkeit offen, historische Anwendungen im Rahmen einer sanften Migration sukzessive auf das neue Backend-System zu überführen.



Governance und Datenschutz

7. Wie steht es um die Governance, speziell den Datenschutz, in einer solchen Hub-and-Spoke Umgebung?

Angesichts der zunehmend strengen Datenschutzvorgaben in der EU und in der Schweiz kommt das Thema Privacy während des Roundtables immer wieder zu Sprache. Moderator Götz Walecki bestätigt den hohen Stellenwert und empfiehlt: Die Benutzerdaten, die in der Regel ja bereits in einer bestehenden Directory-Umgebungen vorhanden sind, sollten im Idealfall physikalisch und logisch durchgehend im entsprechenden Land verbleiben. Das gilt auch (und ganz besonders) für die zugehörigen Passwörter. Die Lösung von Okta greift daher ausschließlich auf vorhandene Bestandsdaten, Basis-User-Objekte und Policy-Integrationen zu und belässt alle erweiterten Attribute und Passwörter durchgehend am ursprünglichen Speicherort. Damit haben Unternehmen auch beim Handling sensibler Kundendaten jederzeit die Gewissheit, sich fest im gesetzlichen Rahmen zu bewegen.

Das Fazit der sechzigminütigen Gesprächsrunde fällt einhellig aus: IAM und CIAM bieten Enterprise-Kunden schon heute viele Möglichkeiten, ihre Prozesse nachhaltig zu optimieren und Kunden, Mitarbeiter und IT-Teams gleichermaßen zu entlasten. Innovative Ansätze wie die Hub-and-Spoke Architektur von Okta ermöglichen es den Verantwortlichen dabei, schon heute die Weichen auf Zukunft zu stellen ohne Abstriche bei der Sicherheit und Compliance in Kauf zu nehmen. Dennoch handelt es sich bei IAM und CIAM in der Regel um anspruchsvolle und tiefgreifende Integrationsprojekte. Kunden sind gut beraten, bei der Planung und Umsetzung erfahrene Integratoren wie iC Consult und die Experten der Hersteller hinzuzuziehen. Diese unterstützen das interne Team mit maßgeschneiderten Beratungs-, Implementierungs- und Integrations-services – und helfen so, einen erfolgreichen Projektverlauf sicherzustellen.